

**1 September 1998**



**Communications and Information**

**COMMAND, CONTROL, COMMUNICATIONS  
AND COMPUTER (C4) SYSTEMS**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the HQ AFRC WWW site at <http://www.afrc.af.mil>. and the AFRCEPL (CD-ROM), published monthly.

---

OPR: 911 AW/SC (Robert Langhurst)  
Supersedes 911 AWI 33-201, 12 September 1997

Certified by: 911 AW/CC (Col F. Baxter Lane)  
Pages: 4  
Distribution: F

---

This instruction implements AFPD 33-2, *Information Protection*. It provides guidance and instructions to all personnel assigned regarding the use and protection of the STU-111. Reference AFI-33-209, *Operational Instruction for the Secure Telephone Unit (STU III) Type I* and Air Force STU-111 Command Authority policy messages.

**SUMMARY OF REVISIONS**

This is a revision of 911 AWI 33-201, 12 September 1997. It updates and streamlines previous guidance.

**1. Responsibilities.** Each STU-III user will ensure the procedures outlined in this regulation are adhered to at all times.

**2. Procedures:**

2.1. When the STU-III is in the unkeyed mode, it will be used to place unsecured unclassified calls only. Removing the CRYPTO Ignition Key (CIK) makes the terminal unkeyed.

2.2. When the terminal is in the keyed mode (CIK in the phone), it must be afforded protection commensurate with the level of the key it contains and may only be used by authorized personnel. When unauthorized personnel are in the area, the keyed STU-III must be under the operational control and within the view of at least one appropriately cleared and authorized person.

2.3. STU-IIIs, not operational 24 hours a day, will have the CIK removed at the close of business. The CIK must be an item on the End-of-Day Security Checklist. The CIK will be stored in a GSA approved security container, if kept in the same room as the STU-III. Only authorized STU-III users will have access to the container. When stored in another room, the CIK will be kept in a GSA approved security containers (if available). If a security container is not available, store the CIK in a

locked cabinet, desk, etc. The adequacy of storage alternatives for the CIK should be determined on a case-by-case basis by the Unit Security Manager within each using organization.

2.4. Strict attention must be paid to the authentication display to ensure the classification level of the conversation does not exceed the highest classification displayed. Recommend users scroll the distant end to ensure the distant end key is current and not expired.

2.5. Before discussing classified information on the STU-III, the person making the classified call must ensure all personnel in the area are cleared and have a need to know.

2.6. Users should pay close attention to the authentication information displayed on the terminal during each secure call. When two terminals communicate in the secure mode, each terminal automatically displays authentication information of the distant terminal. The information displayed indicates the organization reached, the approved level of the call, and when there is foreign access to the terminal, but does not authenticate the person using the terminal. Therefore, users must use judgment in determining when communicating classified information.

2.7. A lost CIK must be reported to the Base COMSEC Custodian immediately. You will be given instructions on what actions to take by the custodian.

2.8. Ensure your equipment custodian has all STU-III assigned to your section listed on the CA/CRL.

2.9. If you experience problems with your STU-III, refer to the operating guide supplied with your STU-III terminal or notify the KMC.

**3. Emergency Action Procedures.** In the event of fire, natural disaster, or covert threat, the CIK will be removed from the phone and locked up or kept in the personal possession of an authorized individual.

**4. Requirements to Install a STU-III in a Residence (on/off the installation).** The unit commander must sign a letter to authorize installation of a STU-III in a private residence (this ensures the Commander knows where the unit's assets are and authorizes government equipment in a private residence). Each person with a STU-III in their residence must contact the Base COMSEC Custodian to receive instructions for use and protection of the STU-III and CIK.

**5.** Each STU-III user must sign an education certification form. This ensures each user understands the security requirements.

F. BAXTER LANE, Col, USAFR  
Commander

**Attachment 1****STU-III EDUCATION CERTIFICATION**

1. When the STU-III is in the unkeyed mode, it will be used to place unsecured unclassified calls only. Removing the CRYPTO Ignition Key (CIK) makes the terminal unkeyed.
2. When the terminal is in the keyed mode (CIK in the STU-III), it must be afforded protection commensurate with the level of the key it contains and may only be used by authorized personnel. When unauthorized personnel are in the area, the keyed STU-III must be under the operational control and within the view of at least one appropriately cleared and authorized person.
3. Strict attention must be paid to the authentication display to ensure the classification level of the conversation does not exceed the highest clearance classification displayed.
4. To ensure that the distant STU-III does not contain an expired key, scroll the distant end STU-III as soon as you go secure. If it does contain an expired key, do not discuss classified information. Call the Base COMSEC Custodian and identify the distant end.
5. Before discussing classified information of the STU-III, the person making the classified call must ensure all personnel in the area are cleared and have a need to know.
6. Each STU-III user must call the Key Management Center (KMC) (1-800-635-6301) once each year to update the firefly key within his or her STU-III. Recommend you call the KMC once a quarter to receive an updated Compromise Information Message (CIM).
7. STU-IIIs, not in operation 24 hours a day, will have the CIK removed at the close of business. The CIK must be an item on the End-of-day Security Checklist. The CIK will be stored in a GSA approved security container if kept in the same room as the STU-III. Only authorized STU-III users will have access to the container. When stored in another room the CIK will be kept in a GSA approved security container. If a security container is not available, store the CIK in a locked cabinet, desk, etc. The adequacy of storage alternatives for the CIK should be determined on a case-by-case basis by the Unit Security Manager within each using organization.
8. If you lose your CIK, notify the Base COMSEC Custodian immediately.
9. The following are reportable COMSEC incidents. They will be reported to the Base COMSEC Custodian:
  - 9.1. Lost STU-III.
  - 9.2. Lost CIK.
  - 9.3. Unauthorized user making a secure call on a STU-III.
  - 9.4. CIK lost and not reported to the COMSEC Responsible Officer or STU-III Responsible Officer (CRO/SRO) within 72 hours.
  - 9.5. Secure call completed using expired key.
  - 9.6. Any instance where the authenticating information displayed during a secure call is not representative of the distant terminal.
  - 9.7. Failure to adequately protect or to erase a CIK associated with a lost terminal.

9.8. Any instance where the display indicates the distant terminal contains compromised key.

9.9. Keyed STU-III (CIK inserted) left unattended, (i.e., no authorized user present for more than five (5) minutes).

9.10. Any instance where the display is inoperative and a secure call is completed.

9.11. Emergency Procedures. In the event of fire, natural disaster, or covert threat the CIK will be removed from the STU-III and locked up or kept in the personal possession of an authorized individual.

---

PRINTED/TYPED NAME OF USER

---

SIGNATURE OF USER